Memorandum

To: Justice Information Board Members and Designees

From: Brian LeDuc, Program Director

Date: 6/10/2004

Re: Report of the Program Director – May 19—June 14, 2004

Proof of Concept Update

The second JIN proof of concept, an exchange of failure-to-appear information among Seattle Municipal Court, AOC and DOL, is now underway. We established connectivity between AOC and DOL on Thursday June 10. The process went smoothly, and it is interesting to note that DIS involvement in the exercise was not required. Attachment 1 is a summary of the project

Summary Offender Profile

The pilot deployment has begun, although no-one from Thurston County appears to be using the application. Additionally, the application has gone down at the time of writing and I have a number of outstanding questions for Templar.

I have also revised and updated the *Quick Start Guide*, which is now the sole source of user help. The document will be posted to the application home page.

Federal Grants for Integrated Justice

At the beginning of this month, the Department of Homeland Security announced that states are eligible to submit up to three proposals that "remove barriers and improve information sharing and integration among public safety agencies." I have collaborated with DOL and WSP to submit a proposal to automate the transfer of firearms licensing information between firearms dealers, local law enforcement agencies and the courts. Attachment 2 is a copy of the proposal.

Strategic Plan

I have spent some more time with the table on page 8 of the JIN strategic Plan, which itemizes the proposed staffing needs of the Program Office. I have set out the requirements in both FTE and dollar units, with the anticipation that the resources would be procured through personal service contracts. Attachment 3 is a copy of the proposal.

Attachment 1

State of Washington

Integrated Justice Information Board

Proof of Concept

DRAFT

S O L U T I O N S I N T I M E

Online Business Systems
One World Trade Center
121 SW Salmon St, 11th Floor
Portland, OR.
97204

Contact: David Neufeld
Phone: 503.221.4517
Email: dneufeld@online-usa.com

TABLE OF CONTENTS

1. Statement of Work

1.1 Solution Architecture

We include the following diagram to represent, in overview, a distributed ESB/Exchange architecture (components and connectivity between components) that we propose for the message exchange of information related to a ***Failure to Appear*** court event between the DOL, AOC, and SMC.

> Note. Representing a change from our originally proposal is that we understand the AOC to be interested in evaluating a web services approach to message production and ESB connectivity.

> Note. Representing a change from our originally proposal is that we understand the DOL to be interested in evaluating both a Java/JMS and a MS .net approach to message consumption and ESB connectivity.

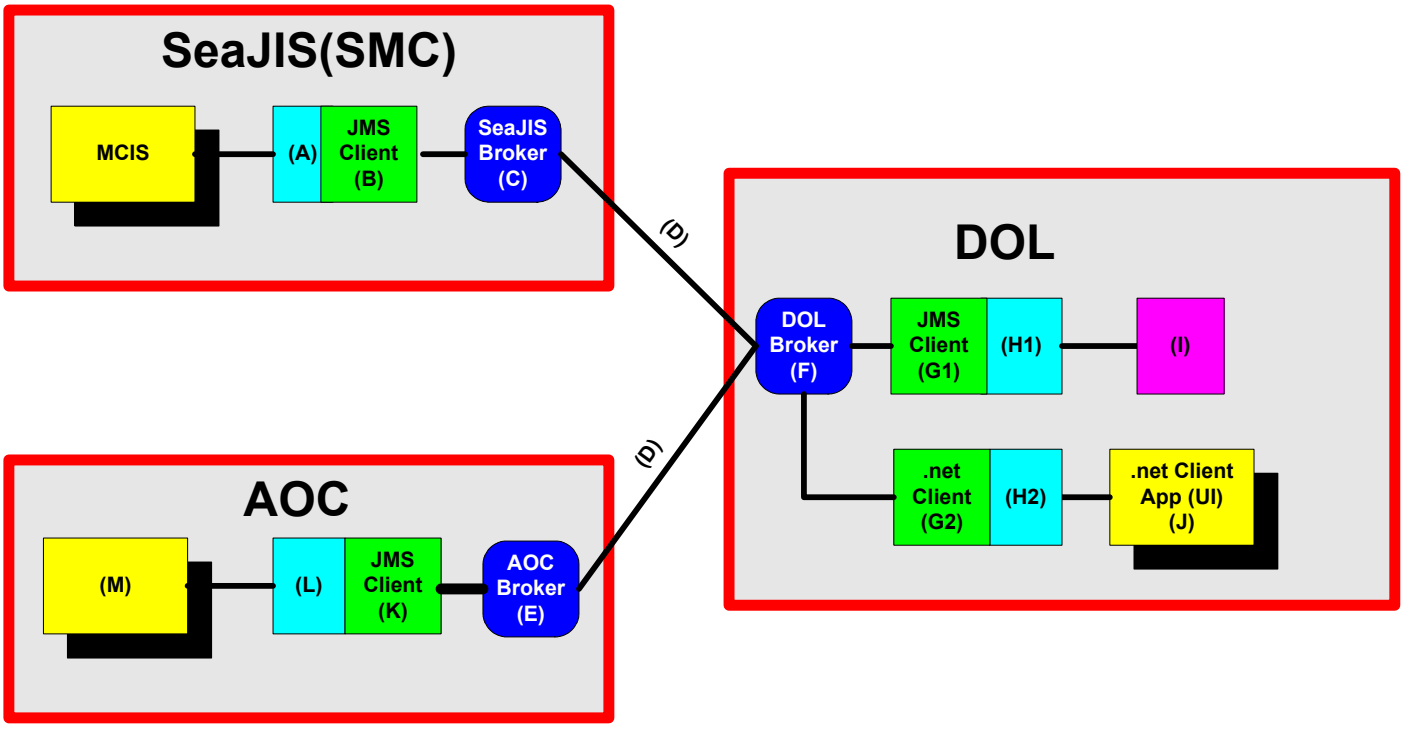


Figure 1 - Solution Architecture

	Solution Architecture Component Description
A	SMC MCIS Connector (Informix JDBC). This component manages the database connection.
B	SMC Producer (Java/JMS). This client creates the messages and places them on the ESB.
C	SeaJIS Sonic Broker (ESB). The broker manages the queues and there message traffic. Online ***assumes*** that this broker will already exist and will be available to the Proof of Concept. Messages will be intelligently routed between the SeaJIS and AOC brokers based on pre-defined routing rules.
D	Connection between brokers and associated routing definitions and security. This includes the Dynamic Routing Architecture built into the ESB.
E	AOC Broker (ESB). The broker manages the queues and Topics and there message traffic.

F	DOL Broker (ESB). The broker manages the queues and Topics and there message traffic.
G1	DOL Consumer (Java/JMS). This client takes the messages off of the ESB to send them to a SQL-Server database (I).
H1	DOL Connector (SQL-Server). This component manages the database connection.
I	DOL Staging Database (SQL-Server). Messages sourced from the SMC or AOC and destined for the DOL will be consumed and inserted into these staging tables. Online ***assumes*** that the DOL end-point will be SQL-Server database tables with schema developed specifically to the proof of concept exchange. Online ***assumes*** the DOL will create and provide access for Online to a SQL-Server database.
G2	DOL Consumer (MS.net). This client takes the messages off of the ESB to send them to a .net UI monitoring application (J).
H2	DOL Connector (MS.net). This component manages the database connection.
J	DOL End-Point Application (MS.net). The .net UI client will provide basic monitoring capability that will allow DOL to visually see messages as they are received. Online ***assumes*** that this is a "temporary" application only and not necessarily subject to the same set of standards and quality assurance rigor of DOL production systems.
K	AOC Producer (Web Service). This client creates the messages and places them on the ESB. Online ***assumes*** that there is a single system ("AOC") from which data will be extracted (produced) and distributed to the DOL.. Online assume the AOC end-point data repository will be a DB2 database. Online assumes the support of AOC application SME in analyzing source data schemas and providing the required access to data.
L	AOC Connector (DB2). This component manages the database connection.
M	AOC Back-office System (DB2)

1.2 Data Architecture

In terms of message content, we assume that the scope of the proof of concept is to include information sourced from both the AOC and SMC end-point systems destined for the DOL related to ***Failure to Appear*** court events.

> ***Assumption – The 80/20 Rule as it relates to JIN PoC Data Architecture.*** We assume that one of the JIN non-technical objectives for the PoC is to demonstrate the function and to understand the functional potential of message exchanges within an ESB implementation. To meet these objectives, we assume that the message structure and content related to Failure to Appear court events must be *complete enough* to be *representative* of a production-ready exchange. Conversely, the message structure and content need not necessarily be fully production-compliant.
>
> This assumption basically strives to constrain effort by considering the ***80/20 Rule***. The 80/20 Rule says that in anything a few (20 percent) are vital and many (80 percent) are trivial. Project Managers know that 20 percent of work (the first 10 percent and the last 10 percent) consumes 80 percent of time and resources.
>
> While difficult to quantify at this juncture, we assume that there will exist a good faith agreement between the project stakeholders and the project delivery team that, to the greatest extent possible, constrains the effort related to data architecture development in consideration of the 80/20 rule. To put it in context – our project plan and estimates have allocated sixty-four (64) hours to the effort of designing a common data format to house information related to Failure to Appear court events sourced from SMC and AOC and destined for DOL.

For the purposes of the Proof of Concept – we propose NOT to develop a common business format between the AOC, DOL, and SMC. Instead, we will have separate and likely unique message formats for each of the SMC-to-DOL exchange and the AOC-to-DOL exchange.

1.3 Server Hardware Specification

The Proof of Concept solution architecture we have proposed requires two (2) servers – one for each of the ESB Brokers located at AOC and DOL. We anticipate the following hardware specification will be sufficient to host these environments for the purposes of the Proof of Concept.

- Fastest Pentium 4 or Xeon processor available
- 2GB of ram [or more]
- 80Gb Hard Drive or more [RAID 5 Configuration recommended]
- 100MBit Ethernet or faster (Redundant Ethernet recommended but optional]
- Redundant Power Supplies [recommended but optional]
- Windows 2000 Server

> ***Assumption – Availability of Broker/Server Hardware.*** We assumed that the servers required to support the Proof of Concept would be made available by JIN or by the AOC or DOL agencies.
>
> If capacity is available on non-Windows / Intel-based servers, Online will review the server specifics together with JIN to determine if they are acceptable.

1.4 Error Handling

Error handling for the POC will be limited in scope to basic error reporting. This will include basic notification via email of ESB errors or issues as well as log files that will keep a history of any error activity and can be searched by authorized users.

This differs from what Online would expect to implement in a full-scale implementation where error handling would be a more full featured implementation included facilities to manage and correct errors that have occurred.

1.5 Security

We assume that the goal of the PoC with regards to security is to adequately protect all in-scope message exchanges and to demonstrate the security features of the architecture. It is not necessarily a requirement of the proof of concept to implement a fully robust production system that implements all available security features of the proposed architecture.

Encryption of the message being transferred over the ESB will be fully implemented and demonstrated as part of the POC. ***Authentication*** and ***authorization*** of users and components will be limited in scope to only those components that required access to the ESB. Additionally, limited access will be granted to the Management Console to specific users.

2. Plan Approach

Requirements and Design

We anticipate collecting requirements and documenting design components in the latter half of April. We anticipate executing this work primarily from our Portland office location.

We propose to gather requirements either by developing survey-style requirement collection forms or thru a series of telephone or on-site interviews. We will then distribute documented requirements to the AOC, SMC, and DOL for review and refinement.

We will use the validated requirements to design the components as described above. Design documents will be distributed to the AOC, SMC, and DOL for review and refinement.

1st Iteration Development

We propose to develop the first iteration of the solution components based on the validated designs from our Portland office location. We anticipate very little involvement will be required from State resources during this phase of activity.

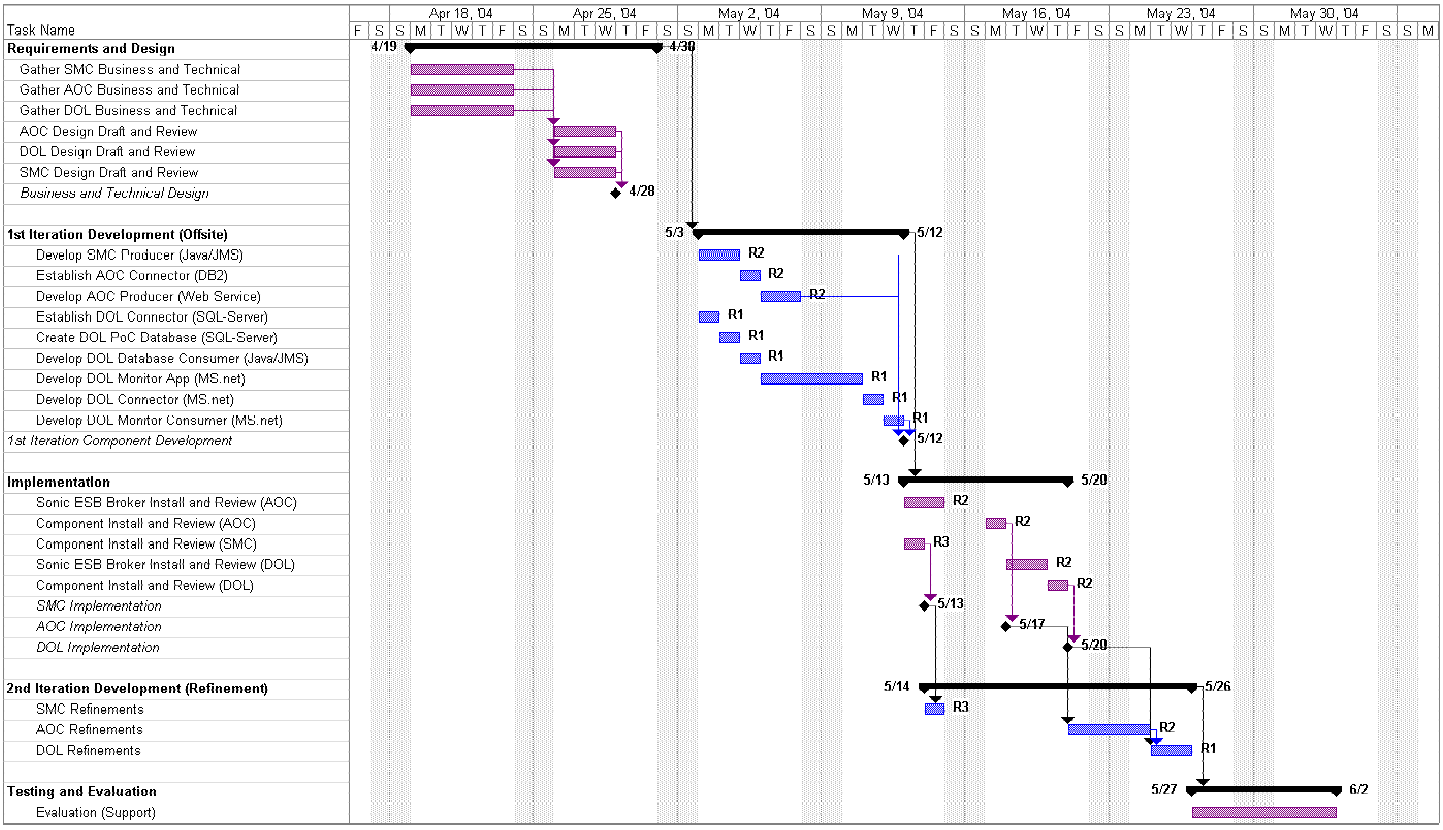
Implementation

The delivery team will install the required Sonic ESB software and then the solution components on location in collaboration with agency/departmental technical staff.

2nd Iteration Development (Refinements)

We anticipate that on-site refinements will be required based on the lessons learned from on-site implementation in the target proof of concept hosting environment.

2.1 Schedule Overview



Public Safety Information Technology Grant Application June 2004

1. Contact Information

William Forth, Firearms Program Manager
Department of Licensing
Wforth@DOL.WA.GOV
(360) 664-6616

Brian LeDuc, Program Director
Justice Information Network
BrianL@DIS.WA.GOV
(360) 902-9889

2. Project Name: Electronic Transfer of Firearms Licensing Information

3. Project participants

AOC	Local Courts	Dept. of Justice
Dept. of Licensing	Local law enforcement	Justice Information Network
Private firearms dealers	WA State Patrol	Private Citizens

4. Statement of the Problem

The Department of Licensing (DOL) proposes development of a Web-based platform to enable:

1) **electronic receipt of criminal conviction and commitment information from the courts;**
2) **pistol transfer forms from firearms dealers; and**
3) **Concealed Pistol and Firearms Licenses from law enforcement agencies.**[1]
4) **Electronic transfer of fingerprints**

This will enhance the public safety value of the program, reduce law enforcement and DOL processing costs, and increase time efficiencies from issuance date to data storage. The current system relies on paper copies of transactions sent to DOL for entry in the firearms system. This process is time consuming, error-prone and duplicates data entry by law enforcement, the courts and firearms dealers into their own databases and into DOL's system.

Firearms dealers are required to send one copy of the pistol transfer form to the law enforcement agency where the applicant resides and a second copy to the DOL within seven days of the sale. Some dealers hold the documents until they have a batch to mail in, often surpassing the seven-day limit. This impedes access to the needed information. Dealers often notify the wrong law enforcement agency because the applicant's mailing address doesn't match jurisdictional boundaries. Additional time is added to the process by mailing and processing time. Often the handwritten forms are illegible, with key information missing.

5. Approach for Conducting Project

The completed project will be incorporated into the DOL operating environment. If courts, firearm dealers and law enforcement agencies send completed documents directly to DOL electronically in a manner consistent with the guidelines and principles of the Justice Information Network, the information will be more accurate and immediately available to law enforcement, who will also be able to retrieve information in more valuable datasets. Strategically, electronic filing will lay a single technological foundation for continuing state efforts to link firearm dealers, law enforcement, DOL, and the courts.

6. Benefits

Aligns directly with National Strategy for Homeland Security[2]
Increased public safety through access to more timely information
Savings through the reduction in printing cost of the current carbon forms
Use of XML standards to achieve integration quickly and efficiently
Collaboration between state, local, federal agencies, private sector
Consistent with state plans for justice integration
Affordable and easily made available to all involved

---

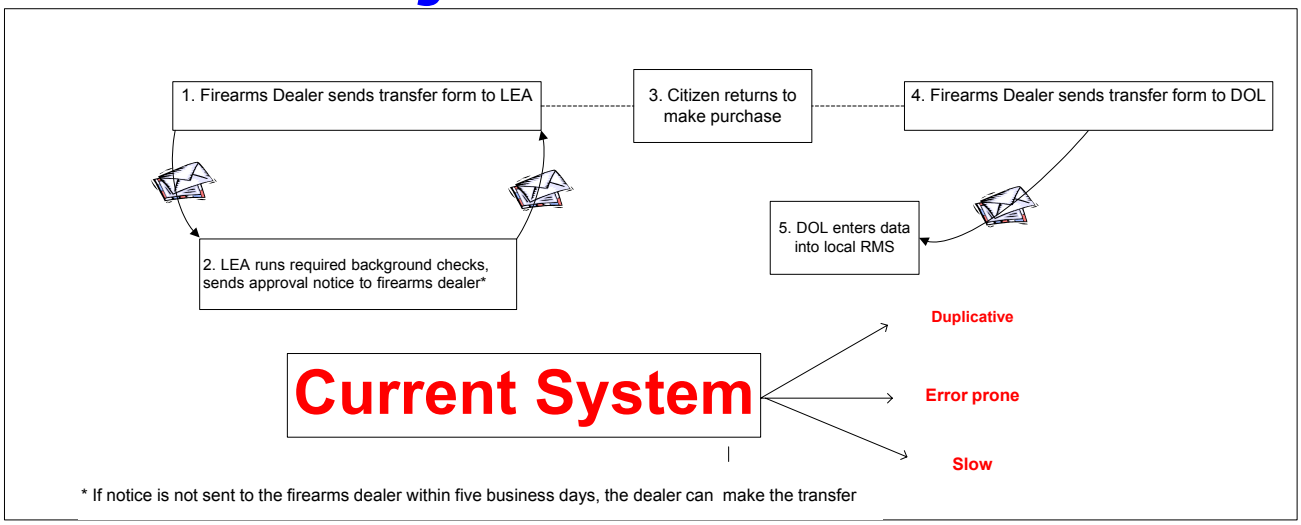
[1] These are all required by law (RCW §9.41.047; RCW §9.41.090; RCW §9.41.070; RCW §9.41.110)

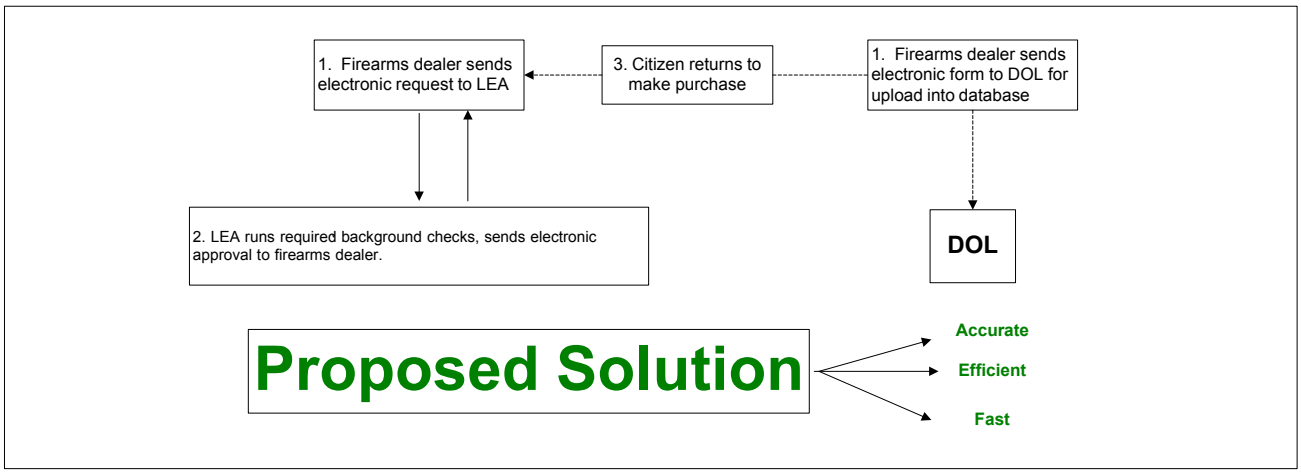
[2] Office of Homeland Security, *National Strategy*, 2002, pp. 26, 33, 48, 57.

Budget

Contractor Development Costs	$600,000
Server software	$50,000
User Authentication Tools	$25,000
Live Scan Devices for LEAs (5)	$150,000
Training	$50,000
Agency Overhead (7%)[3]	$121,300
Total	**$996,300**

Project Overview





[3] Includes I/S overhead of 4%, Project QA (10%)

Attachment 3

JIN Program Office		
Role	**Responsibility**	**FTE**
Program Director	Provide executive level direction and serve as the Chief Executive Officer for JIN; Prepare strategic plans and budgets for justice integration projects; Research and aggressively seek funding; Coordinate technical staff in support of JIN projects and applications; Coordinate JIN project activities with agency/law enforcement project managers and resolve technology issues related to sharing data; Lead subcommittees and workgroups in developing and implementing standards, both technical and business practice.	1.0
Technology Officer	Maintain JIN technical standards Develop and maintain JIN portfolio Develop re-usable templates for JIN constituents	0.4
Project Manager	Oversee support operations Manage JIN projects (SOP, network)	0.25
Communications	Develop and maintain JIN website Build JIN knowledge base Produce JIN newsletter Oversee awareness efforts	0.5
Procurement/Legal	Provide assistance with contracts, agreements, procurement Review software licensing agreements Update RCW Charge Table Research and counsel	0.1
Finance	Budget assistance	0.1
Grants	Identify and circulate grant opportunities Grant-writing assistance	0.2
Administrative Support	Manage Director's schedule and cost center General administrative support Process travel expenses for Board members	0.3
Technical Support	Support Summary Offender Profile, other projects Security patches, backup, etc.	0.25